# Thoughts about Mordell and Uniformity of finiteness bounds

*Mordell 2022 Lectures*

Barry Mazur

# Mordell

# BEATS THE WORLD AT MATHEMATICS

LEWIS J. MORDEL

Lewis J. Mordel, High School Graduate, Wins Scholarship in Cambridge Over Competitors from Many Countries.

Lewis J. Mordel, a graduate of the Central High School, brought additional honors to his alma mater yesterday, when he was awarded a three-year scholarship in mathematics by St. John's College, Cambridge, England.

Mordel went to Cambridge with nothing but his High School training and competed against graduates of schools and colleges in every part of the world. The examinations were open to all competitors, but for the first time a High School graduate was entered against college men. His entry created laughter instead of serious consideration, but at the conclusion of the examinations, which lasted four days, he stood No. 1 of 250 applicants, with an average of a trifle below 100.

At the Central High School Mordel's ability along mathematical lines was regarded by the members of the faculty as phenomenal. In his Sophomore year he had completed the mathematical course provided for the four-year course and during his last two years in the school he took up the higher mathematics.

To support himself he devoted seven hours of every day to coaching his fellow-students, and on one occasion stood at a blackboard for forty-eight hours in an endeavor to pull a student through an examination. And the examination was passed. At the end of his Senior year he devoted all his time to coaching, having no examinations to take, and in this manner earned enough money to take him to England.

Mordel's present aim is to cover his three years' work sufficiently well to entitle him to a fellowship for four additional years.

# Concrete questions

One striking aspect of Mordell's mathematics is how he is known both for the *concrete questions* posed in simple English sentences that he considered, such as:

Which products of two consecutive integers are also products of three consecutive integers?

The answer: 0,6, and 210

# Or

Given an integer $n$, in how many ways can it be expressed as the difference between a square and a cube? (And the same question given a rational number.)

# And, in contrast: Mordell's general theorem

*that the group of rational points of an elliptic curve over* $\mathbb{Q}$ *is finitely generated*

—a theorem generalized by André Weil to cover abelian varieties over number fields.

And his broad conjecture *that curves of genus* $> 1$ *over* $\mathbb{Q}$ *have only finitely many points*

—proved four decades ago by Faltings over general number fields,

with further proofs coming from different angles,

by Vojta, Bombieri, and Faltings again; and a very recent proof (2020) by Lawrence, and Venkatesh.

# *Related work, extending Mordell's Conjecture:*

There is a long list of fundamental results extending his Conjecture[1] and, e.g., bounding division points on subvarieties of semi-abelian varieties[2].

*. . . comment about footnotes. . .*

[1] See my survey article *Abelian Varieties and the Mordell-Lang Conjecture* in Model Theory Algebra and Geometry, MSRI Publications **39** (2000) 199-227.

[2] e.g., McQuillan, Michael (1995). "Division points on semi-abelian varieties". Invent. Math. 120 (**1**): 143-159

The hundredth anniversary of Mordell's foundational paper, proving his famous theorem and posing his famous conjecture

is a good moment to review some basic questions it opened up: questions of finiteness and uniformity in arithmetic.

# Uniformity of Mordell-Weil rank

To begin, consider this fairly recent (striking!) conjecture[3] suggested by computations that depend on the random matrix heuristic. It is striking in its precision, and in how close it is to the data accumulated so far.

[3] *A heuristic for boundedness of ranks of elliptic curves*, Jennifer Park, Bjorn Poonen, John Voight, Melanie Matchett Wood
https://arxiv.org/abs/1602.01431

## Conjecture

*(Park, Poonen, Voight, Wood) There are only finitely many elliptic curves over $K = \mathbb{Q}$ of Mordell-Weil rank greater than* 21*.*

We know, in fact, very few examples of Mordell-Weil rank greater than 21. Here's one:

# Noam Elkies' elliptic curve "$E_{28}$"

of rank $\geq 28$ :

$$Y^2 + XY + Y = X^3 - X^2 -$$

$$-20067762415575526585033208 \sim$$

$$\sim 209338542750930230312178956502X +$$

$$+3448161179503055646703298569039072037485594 \sim$$

$$\sim 4435931918036126600829629193944873224342 9.$$

and it is of rank exactly 28 subject to GRH[4].

[4] Klagsbrun, Sherman, and Weigandt
https://arxiv.org/pdf/1606.07178.pdf

## An impressive amount of recent and current work—within the past two pandemic years!

has been devoted to *uniformity issues* regarding numbers of points having various interesting properties on curves (and on higher dimensional varieties).

Work, for example, of:

De Marco-Krieger-Ye,
Dimitrov-Gao-Habegger,
Gao-Ge-Kühne,
and very recent work of Kühne,
and others. . . .

# Although I won't have time to do justice to even any one of these exciting developments,

I will at least hint at their existence, giving me the opportunity to ask yet more uniformity questions.

The thrust of Mordell's classical conjecture is that it suggests (i.e., it conjectures) that a purely diophantine consequence follows from a purely (algebraic) geometric hypothesis.

Later, and in a broader context, Serge Lang adopted this attitude toward the relationship between arithmetic and geometry, to frame his more general conjectures.

# Abuse of Language

Below I'll be dealing with abelian varieties over fields $K$ and abelian schemes over base schemes $S$. But I will abuse the terminology a bit by calling an

"abelian variety"

any variety (of positive dimension) that becomes an abelian variety over some finite degree extension field $L$ of $K$ after the choice of a rational point as 'origin.'

And, in the case where the base scheme is $S$ I'll call it an abelian scheme over $S$ if it becomes an abelian scheme over $T$ after some finite flat base change $T/S$ and the choice of a $T$-section, as 'section of the origin.'

# (Following Serge Lang)

An algebraic variety (say: smooth, projective, geometrically irreducible) over a finitely generated field $K$ is called

**Mordellian**

if $V$ has only finitely many $L$-rational points over any extension $L/K$ of *finite degree*.

# I'm using the neologism *Mordellian*

because Lang's concept of

**Mordellic**

requires that $V$ have only finitely many rational points over any *finitely generated* extension of $K$ whereas my definition requires that it have only finitely many points over any extension of $K$ of *finite degree*.

*Since I haven't checked yet that these boil down to the same thing, I need a different term.*

## We have a classical theorem and a classical conjecture regarding this Lang-like notion

First, the Theorem (Faltings): If $V_{/K}$ is

**(1)** a subvariety of an abelian variety over a number field $K$

**(2)** that doesn't contain any subvariety that is an abelian variety,

then $V$ is Mordellian.

## For curves $V$, this reduces to... the classical Mordell Conjecture:

A curve $V$ over a number field $K$ satisfying the first condition is not of genus 0 and satisfying the second is not of genus 1, so the theorem establishes an equivalence:

A curve (smooth, projective, geometrically irreducible) is Mordellian if and only if it satisfies (1) and (2) above.

# Second, the conjecture

perhaps due to—but in any event, in the style of—Serge Lang):

A variety $V$ as above is Mordellian if and only if it doesn't contain a nontrivial image of

1. a rational curve, or
2. an abelian variety,

# A related conjecture also attributed to Lang:

**Conjecture ( "The Strong Lang Conjecture" (SLC))**

*For $X$ a variety of general type, defined over a number field $K$*

*there is a proper subvariety*

$$Z \subset X$$

*whose complement $X \setminus Z$ is Mordellian.*

# Mordellian schemes

It is natural to broaden the definition of 'Mordellian' over any base scheme $S$—but, to focus the mind a bit:

let $S$ be a regular connected scheme of finite type and the structure morphism

$$f : V \to S$$

a smooth faithfully flat extension, with $V$ also connected.

## Definition

The $S$-scheme $V_{/S}$ is **Mordellian** if for every finite flat morphism $T \xrightarrow{\iota} S$ the base changed scheme

$$V_{/T} := V_{/S} \times_S T$$

has only finitely many $T$-sections.

# A classical example

**Theorem**

*Let $S := Spec(\mathcal{O}_K)$ where $K$ is a number field and*

$$V_{/S} = \mathbb{P}^1_{/S} \ \setminus \ D$$

*where $D$ is a divisor on $\mathbb{P}^1_{/S}$ given by the support of the zeroes of a homogeneous polynomial*

$$f(x,y) \in \mathcal{O}_k[x,y]$$

*of degree $\geq 3$, with the gcd of its coefficients equal to $1$, and having no multiple roots. Then $V_{/S}$ is Mordellian.*

# The very classical example is:

$$f(x, y) = xy(x - y)$$

where the $S$-sections are given by pairs of units of $\mathcal{O}_K$ that sum to 1. There are only finite many such, by Siegel's Theorem.

# Uniformity—useful, and less useful—of finiteness bounds

For a useful definition of *height* we can fix on any positive real valued function of the coordinates that has the property that for any fixed number field $K$ the number of coordinates $(x_1, x_2, \ldots, x_\nu)$ of height bounded by a real number $X$ is finite.

If you have a proof that the set of solution of a system of polynomial equations is finite and the algorithm provided by the proof offers an upper bound for the *heights* of the solutions,

in principle (if not in practice) just setting a computer going—

to systematically climb coordinates with greater and greater heights up to the upper bound

—gives you all the solutions.

If your proof only offers an upper bound for *the number* of solutions, this is far less helpful, because the upper bound provided by the proof (for the *number* of solutions) is often strictly larger—usually astronomically larger—than

the actual number of solutions[5].

So—just by having such an inexact upper bound for the number of solutions— even if you systematically search, you may never know whether you have a complete set.

[5] A few years ago I learned that Model Theory provided a proof of finiteness of the number of points with a certain property that interested me. I asked Tom Scanlon and James Freitag for the upper bound that the Model Theoretic proof provided. It was striking that this bound can be computed; it was $36^6$. I'm guessing, though, that the actual number is something like 3 or 4.

# *All known proofs of Mordell's Conjecture*

do provide upper bounds for the number. . .
but not for the height of rational points on curves of genus $> 1$.

# Classical questions regarding finiteness and uniformity of upper bounds

At least three "named problems" have been the subject of recent results regarding uniformity[6]:

- The "second part of Hilbert's 16th Problem
- The Uniform Mordell-Lang Conjecture over $\mathbb{C}$
- The Manin-Mumford Conjecture

[6] I want to thank Dana Schlomiuk, Umberto Zannier and Ziyang Gao for conversations we had about different aspects of this, as I was preparing my slides.

# The "second part of Hilbert's 16th Problem"

The problem, as posed by Hilbert at the International Congress of Mathematicians in 1900, is, in effect, to show that the number of limit cycles for any planar vector field defined by

$$\frac{\partial x}{\partial t} = P(x, y); \qquad \frac{\partial y}{\partial t} = Q(x, y)$$

where $P(x, y), Q(x, y) \in \mathbb{R}[x, y]$ are polynomials of degree $n$

is finite... and is less than a bound that only depends on the degree $n$—possibly a polynomial in $n$.

## (The status of Hilbert's 16th Problem problem at the moment is interesting!)

Steve Smale's comment: about this problem: "Except for the Riemann Hypothesis, it seems to be the most elusive of Hilbert's problems."

# The Uniform Mordell-Lang Conjecture

For a discussion of this and related problems, see

- Marc Hindry's (1997) *Introduction to abelian varieties and the Mordell-Lang Conjecture* `https://webusers.imj-prg.fr/~marc.hindry/abvarmodel.pdf` over $\mathbb{C}$

and

- two wonderfully extensive reviews by Ziyang Gao (2021), including very recent work by Dimitrov, Habegger, Gao, Ge, and Kühne on Uniform Mordell-Lang—
  - *A proof of the Uniform Mordell-Lang Conjecture* `https://webusers.imj-prg.fr/~anna.cadoret/uml_complete.pdf`
  - Recent developments of the Uniform Mordell-Lang Conjecture. arXiv:2104.03431, April 2021

# The Uniform Mordell-Lang Conjecture

The classical Mordell Conjecture is, of course, *arithmetic*: it is about $K$-rational points when $K$ is a number field.

But the most general form of the Uniform Mordell-Lang Conjecture is over $\mathbb{C}$—it is, in effect, complex analytic: it is a question about algebraic varieties over $\mathbb{C}$.

# Uniform Mordell-Lang Conjecture(s)

Uniform Mordell-Lang Conjecture**s** mean ('uniform' versions of) Mordell's classical conjecture with uniformity bound dependent on various things *and especially that interesting extra variable:*

$$\rho := \text{the Mordell-Weil rank of the jacobian.}$$

($\rho$ being appropriately interpreted)

# The *uniformity* being:

an upper bound for the number of $K$-rational points of a curve $C$ of genus $g > 1$ with jacobian having Mordell-Weil rank $\rho$ over $K$, the upper bound having the form:

$$B^{1+\rho},$$

*and where one can take the constant $B$ to be only dependent on:*

- $g, [K : \mathbb{Q}]$, and the Falting height of the jacobian of $C$.

  ($\sim$ 1995) Vojta, Faltings, Bombieri, de Diego, David-Philippon, and Rémond.

- $g$ and $[K : \mathbb{Q}]$

  (2021)V. Dimitrov, Z. Gao, and P. Habegger

- $g$ alone! (which 'allows for' a generalization entirely in the vocabulary of complex analytic varieties)

  (2021) L. Kühne[7]

[7] Equidistribution in Families of Abelian Varieties and Uniformity, arXiv:2101.10272

With corresponding uniformity properties proved about subvarieties of abelian varieties not containing abelian varieties. . . rather than just curves.

As in recent work of Z. Gao, T. Ge and L Kühne establishing:

The Uniform Mordell-Lang Conjecture
(and the Uniform Bogomolov Conjecture)

for subvarieties of abelian varieties.

But, back to curves:

# Moving the Problem from Diophantine vocabulary to complex analytic vocabulary

Say that a group $\Gamma$ is of **(finite) rank** $\rho$ if

$$\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$$

is a $\mathbb{Q}$-vector space of dimension $\rho$.

## Question

*Given an algebraic curve over $\mathbb{C}$ of genus $g > 1$ embedded in its jacobian $J$ and a subgroup $\Gamma \subset J(\mathbb{C})$ of rank $\rho$ is there a uniform upper bound—$B(g, \rho)$ (dependent only on $g$ and $\rho$) for the number of points in the intersection of the curve and $\Gamma$?*

Note that if one proves that there is such a bound, $B(g, \rho)$, for finitely generated subgroups $\Gamma \subset J(\mathbb{C})$,

this same bound $B(g, \rho)$ works, bounding $|\Gamma \cap C|$ for all subgroups $\Gamma \subset J(\mathbb{C})$ of rank $\rho$.

**Proof.**

Any such group $\Gamma$ is a union of a nested sequence

$$\Gamma_1 \subset \Gamma_2 \subset \ldots \Gamma_n \subset \Gamma = \cup_{n=1}^{\infty} \Gamma_n$$

each $\Gamma_n$ a finitely generated subgroup, each of rank $\rho$, and hence each of these contain at most $B(g, \rho)$ points of $C(\mathbb{C})$. $\square$

## The Uniform Mordell-Lang conjecture is that the answer to this question is YES.

A proof of this conjecture has very recently been submitted to Archiv by Lars Kühne. And the bound can (again!) be taken to be

$$B(g, \rho) = B(g)^{1+\rho} \qquad (1)$$

for $B(g)$ a function of the genus alone.

# The Uniform Mordell-Lang Conjecture over $\mathbb{C}$ includes both:

1. The classical Mordell Conjecture

and

2. The Manin-Mumford Conjecture.

We will return soon to these uniformity issues regarding rational points on curves of genus $> 1$, but now:

# The Manin-Mumford Conjecture

Yuri Manin and David Mumford posed (independently) the following question:

Does any curve of genus $> 1$ when viewed as a subvariety of its jacobian contain only finitely many torsion points?

This question—answered affirmatively by Raynaud in 1983 —has many variants; e.g.,

## Conjecture

(**Manin-Mumford**) *Any injective morphism of a curve of genus* $> 1$ *into an abelian variety has only finitely many torsion points of the abelian variety in its image.*

# or more general formulations due to Bogomolov;

Bogomolov conjectured that for any $\epsilon > 0$ such a curve has only finitely many algebraic points that are (as the curve sits in its Jacobean) within $\epsilon$ of a torsion point—as measured by Néron-Tate height.

These questions have been answered by results of Ullmo (using work of Szpiro and Zhang).

And further general statements about subvarieties of abelian varieties have been proved by Zhang.

# Uniform Manin-Mumford

In recent years we have begun to see striking *uniformity* results regarding this Manin-Mumford question (and the corresponding Bogomolov question).

For example In 2020 De Marco, Kreiger, and Ye proved uniformity of bounds for bielliptic curves.

Lars Kühne (last year) established the Uniform Mordell-Lang Conjecture over $\mathbb{C}$ and this includes the full Uniform Manin-Mumford Conjecture;

i.e., the existence of a uniform upper bound $B(g)$ for the number of torsion points of the jacobian that lies on a curve (of genus $> 1$ ) embedded in it.

# And this morning, Ziyang Gao gave a sketch of a proof of his recent work with Habegger on the relative uniform Manin-Mumford problem.

This is the *Manin-Mumford* version of the the Relative Bogomolov Conjecture [8].

This new result uses the Pila-Zannier method, with many of the techniques having appeared in Dimitrov-Gao-Habegger's proof of their version of uniform Mordell-Lang.

[8] (Conjecture 10.1 of Gao's survey `https://webusers.imj-prg.fr/~ziyang.gao/articles/SurveyUnifML.pdf`

# *Other* types of *uniformity* of upper bounds for the number of rational points on curves of genus $g$

Here are three other uniformity formats that are qualitatively different *uniform* upper bounds for the number of rational points of curves of genus $g$ with jacobians of rank $\rho$ over number fields of degree $d$.

- **(1)** A *Chabauty-Kim bound:* These bounds are in the format of Minhyong Kim's extension of Robert Coleman's way of extending the classical method of Chabauty. Chabauty's method requires that $\rho < g$.

  Adopting the Chabauty-Kim framework, Jennifer Balakrishnan in various publications e.g., with A. Besser, and J. S. Müller [9] and with Netan Dogra [10](and others) provide "Quadratic Chabauty" bounds when $\rho = g$.

---

[9]Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves. J. Reine Angew. Math., 720:51- 79, 2016

[10]An Effective Chabauty-Kim Theorem `arXiv:1803.10102v2`

These bounds are (usually) only over the field $\mathbb{Q}$ but they are given with explicit (usable) constants and where the rational points are among the zeroes of a specified analytic function.

Regarding uniformity, see forthcoming work (*Towards Uniform Chabauty-Kim*) by L.A. Betts, D. Corwin, and M. Leonhardt giving explicit bounds for the number of rational points on curves of genus $g$ over $\mathbb{Q}$ where the bounds are in terms of $g$, $\rho$, and and certain numbers related to the reduction type of the curve at primes of bad reduction.

- **(2)** *Statistical bounds:*

Enormous progress has been made in recent years in establishing *average* bounds.

E.g., as in the work of Manjul Bhargava and Benedict H. Gross, Bjorn Poonen and Michael Stoll, Arul Shankar and Xiaoheng Wang, and Levent Alpoge.

- **(3)** A (conjectured) bound *independent of the number field, or $\rho$!*

... except for finitely many "exception curves"—the number of these *exceptions* being dependent of the number field.

Lucia Caporaso, Joe Harris and I conjecture that for any genus $g > 1$ there is a finite upper bound $N(g)$ such that:

for any number field $K$ there are only finitely many (isomorphism classes over $K$) of curves of genus $g$ defined over $K$ with more than $N(g)$ $K$-rational points.

This may seem a bit extreme, however we've proved that the above conjecture follows from the Strong Lang Conjecture.

. . . *Comment about the published proof (1997)!. . .*

But see:

L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points: an up-date and corrections*, Tunisian Journal of Mathematics **4** (2022), No. 1, 183-201

# Behavior of $N(g)$ as $g$ tends to $\infty$

Given $g$, for $n = 2g + 2$ consider the hyperelliptic curves

$$C: \quad Y^2 = (X - a_1)(X - a_2) \cdot \cdots \cdot (X - a_n)$$

with $a_i \in \mathbb{Q}$ ( for $i = 1, 2, \ldots, n$ with $a_i \neq a_j$ if $i \neq j$).

Such a curve $C$ is of genus $g$ and since

$$\{(0, a_i) \quad | i = 1, 2, \ldots, n\}$$

is a subset of its $\mathbb{Q}$-rational points, we have

$$|C(\mathbb{Q}| \geq n.$$

Moreover by varying the $a_i$ we get infinitely many such curves defined over $\mathbb{Q}$—and non-isomorphic, even over $\mathbb{C}$.

So,

$$N(g) \geq 2g + 2.$$

# Automorphism orbits of rational points

For $C$ a smooth projective, irreducible curve of genus $g > 1$ defined over a number field $K$ let $Aut_K(C)$ be the group of automorphisms of $C$ defined over $K$.
The group $Aut_K(C)$ acts naturally on the set $C(K)$ of $K$-rational points of $C$.

Let $\nu(C; K)$ denote the number of $Aut_K(C)$-orbits in $C(K)$ under that natural action.
So, of course,

$$\nu(C; K) \leq |C(K)|$$

and therefore any uniform upper bound established for $|C(K)|$ is valid for $\nu(C; K)$ as well.

Define $\nu(g)$ to be the smallest integer that has the property that for each number field $K$ there are only finitely many curves $C$ of genus $g$ defined over $K$ with the property that $\nu(C; K)$ is strictly greater than $\nu(g)$.

So:

$$SLC \implies \{\nu(g) < +\infty\}$$

If one feels that there is a fair chance for SLC to be true, and hence for $\nu(g)$ to be finite, one might wonder about the asymptotic behavior of $\nu(g)$ as $g$ tends to infinity.

Needless to say, we have no real evidence to make any conjectures, or precise predictions, but:

### Question

*Is*

$$\nu(g) = 3g + o(g)?$$

*. . . discuss. . .*

# Uniformity of dimension of the 'Diophantine span' of moduli spaces

Here is yet another type of diophantine *uniformity*:

Definition

For $V$ a variety over $K$ a number field, the $K$-**Diophantine span** of $V$ is the dimension of the Zariski-closure in $V$ of the set $V(K)$ of $K$-rational points of $V$.

...also for stacks...

# Consider the moduli stack $M_{g,n}$

of curves of genus $g$ with an ordered system of $n$ designated points.

Let

$$M^*_{g,n} \subset M_{g,n},$$

be the substack of curves of genus $g$ with an ordered system of $n$ *distinct!* points

And let $d_{g,n}(K)$ denote the $K$-diophantine span of

$$M^*_{g,n}$$

Now ‘quantify over all number fields” and define:

$$d_{g,n} := \max_K d_{g,n}(K).$$

# Uniformity in $n$?

Fix $g > 1$.

*The trivial upper bound:*

$$d_{g,n} \leq 3g - 3 + n$$

SLC $\implies$ If $n \gg_g 0$—then $d_{g,n} = 0$.

# What else can one say (or conjecture) about these $d_{g,n}$?

**Query**

*Can one find an example where $d_{g,m} > d_{g,n}$ with $g > 1$ and $m > n$?*

E.g., consider $d_{2,n}$ for varying $n$?

Is $d_{2,n} = 3$ for $n \leq 7$.

**Query**

*What can be said about the asymptotic of $d_{g,0}$ for varying $g$?*

Lots to be thought about... following the spirit of Mordell!